INTELLIGENT TOKEN PROTECTED SYSTEM WITH NETWORK AUTHENTICATION

FIELD OF THE INVENTION

The present invention relates to the computer security field. More particularly, the present invention relates to a network authentication system and method using an intelligent token.

BACKGROUND OF THE INVENTION

Security is a particularly vexing problem in the computer industry. Users often perform sensitive applications and tasks on their computers and they are desirous of maintaining confidentiality with respect to their information and data. In computer systems, it is common to use a firewall to separate various segments of a network.

As defined herein, a firewall is a bastion host which separates administrative domains. An administrative domain may be a single computer or a network of computers. For example, in a conventional computer system, a firewall may be utilized to separate a local area network from a wide area public network, e.g., the Internet. Firewalls may also be used to secure an intranet domain against unauthorized access. For example, in a large corporate environment, the firewall may separate the local corporate net from a dedicated segment used by one of the corporate departments.

Firewalls physically separate administrative domains. All traffic from one domain (the local domain) that is directed to a second domain (the remote domain) must pass through the firewall. Thus, if a user operating from the local domain would like to communicate with the remote domain, the user must communicate through the firewall.

User authentication to the firewall is required in order to communicate with the remote domain. Authentication is a check to ensure that the user is authorized to have access to a given device, e.g., an intelligent token, a computer, etc. Existing systems authenticate users through the use of reusable passwords or challenge-response techniques. In a password based system, after the user has "booted" a local host computer, the user requests a connection to a remote host computer, provides a user identifier and, when prompted, provides a password. Successive authentications use the same user identification and password. Hence, an attacker who misappropriates a user password is able to easily and continuously gain access to the remote host, and, thus, the remote domain.

In a challenge-response system, the remote host requests a user identifier and issues a challenge to the user. The user calculates a response which, if deemed valid by the remote host, grants access to the remote host. Because the challenge changes for successive authentications, the challenge-response method is not vulnerable to password misappropriation as described above. However, responses to the challenges must be computed. They may be computed 1) manually, 2) by the local host using software methods or 3) by a portable hardware device. In each of the three cases, the user is required to manually enter the calculated response. In many systems, the user must also enter the challenge.

It is readily apparent from the above described procedures that in order to communicate with the remote domain, the user is required to remember extensive information regarding the system and provide substantial input to the system. The user must know and input the required information to boot the local host computer. Further, the user must input additional information to access the remote host. Hence, there is need for a system that allows the user secure access to remote domains with minimal information input.

SUMMARY OF THE INVENTION

In accordance with an aspect of the invention, an intelligent token is provided which stores critical information including authentication information. A local host computer is coupled with the intelligent token such that the local host computer communicates authentication information with the intelligent token. After the local host computer has been authenticated, the local host computer communicates authentication information to a remote host computer without input from the user. The remote host computer is then authenticated.

In a preferred embodiment of the invention, the intelligent token sends a request for access to the remote host computer and the remote host computer sends a challenge to the intelligent token in response. The challenge is stored in the memory of the remote host computer. The intelligent token generates a response to the challenge and the response is verified by the remote host computer using the stored challenge thus allowing free communication between the intelligent token and the remote host computer.

In accordance with another aspect of the invention, the intelligent token includes a CPU and first and second memory units. The first memory unit stores an operating system. The second memory unit stores critical information including host and remote authentication information such as cryptographic keys and file signature information. The authentication information may include host and remote access codes.

A particularly advantageous feature of the invention is that the local host computer and the remote host computer are authenticated with no more user input than is necessary to authenticate the intelligent token. Thus, the system is securely insulated from attack because the authentication information is stored in the intelligent token.

Yet another advantageous feature of the invention is that it facilitates a secure boot for the local host computer and automatically authenticates the remote host computer to the intelligent token without further input from the user.

Still another advantageous feature of the invention is that it provides a virus check for files stored on both the remote and host computers.

An additional advantageous feature of the invention is that it facilitates encrypted communication between the local host computer and the remote host computer.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram illustrating the local host computer coupled to the remote domain.

FIG. **2** depicts the intelligent token.

FIG. **3** shows is an enlarged view of the memory of the intelligent token.

FIG. **4** is a block diagram of the local host computer.

FIG. **5** is a flowchart describing the boot and authentication processes from the perspective of the local host computer.

FIG. **6** is a flowchart describing the boot and authentication process from the perspective of the intelligent token.

FIG. **7** is a flowchart illustrating the remote domain authentication process.

DETAILED DESCRIPTION OF THE EMBODIMENTS

The present invention is an improvement to the invention described in U.S. Pat. No. 5,448,045 which is incorporated